ANATOMY OF TORSION IN THE CM CASE

ABBEY BOURDON, PETE L. CLARK, AND PAUL POLLACK

Abstract. Let $T_{\mathrm{CM}}(d)$ denote the maximum size of a torsion subgroup of a CM elliptic curve over a degree d number field. We initiate a systematic study of the asymptotic behavior of $T_{\mathrm{CM}}(d)$ as an "arithmetic function". Whereas a recent result of the last two authors computes the upper order of $T_{\mathrm{CM}}(d)$, here we determine the lower order, the typical order and the average order of $T_{\mathrm{CM}}(d)$ as well as study the number of isomorphism classes of groups G of order $T_{\mathrm{CM}}(d)$ which arise as the torsion subgroup of a CM elliptic curve over a degree d number field. To establish these analytic results we need to extend some prior algebraic results. Especially, if $E_{/F}$ is a CM elliptic curve over a degree d number field, we show that d is divisible by a certain function of $\#E(F)[\mathrm{tors}]$, and we give a complete characterization of all degrees d such that every torsion subgroup of a CM elliptic curve defined over a degree d number field already occurs over $\mathbb{Q}$.

Contents

1. Introduction

1.0. **Terminology, notation and conventions.** Throughout, ℓ denotes a prime number. We say ℓ^α *exactly divides* n, and write $\ell^\alpha \parallel n$, if $\ell^\alpha \mid n$ but $\ell^{\alpha+1} \nmid n$. We use the notation $\omega(n)$ for the number of distinct primes dividing n, and we write $\Omega(n)$ for the number of primes dividing n counted with multiplicity.

2010 *Mathematics Subject Classification.* Primary: 11G15; Secondary: 11G05, 11N25, 11N37.

If K is a number field, we let $\mathcal{O}_K$ denote its ring of integers, Δ_K its discriminant, h_K its class number, and w_K the number of roots of unity lying in K. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we denote by $K^{(\mathfrak{a})}$ the $\mathfrak{a}$-ray class field of K.

We say an elliptic curve E over a field of characteristic zero has $\mathcal{O}$-CM if $\mathrm{End}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field K. The statement "E has K-CM" means that E has $\mathcal{O}$-CM for some order $\mathcal{O}$ in K.

The *torsion rank* of a finite abelian group G is the minimal number of elements required to generate G.

Let $\mathscr{A}$ be a subset of the positive integers. We define the *upper density*

$$\overline{\delta}(\mathscr{A}) = \limsup_{x\to\infty} \frac{\#\mathscr{A} \cap [1,x]}{x}$$

and the *lower density*

$$\underline{\delta}(\mathscr{A}) = \liminf_{x\to\infty} \frac{\#\mathscr{A} \cap [1,x]}{x}$$

When $\overline{\delta}(\mathscr{A}) = \underline{\delta}(\mathscr{A})$, we denote the common quantity by $\delta(\mathscr{A})$ and call it the *asymptotic density* of $\mathscr{A}$.

1.1. $T(d)$ **versus** $T_{\mathrm{CM}}(d)$**.** A celebrated theorem of L. Merel [25] asserts that if E is an elliptic curve defined over a degree d number field F, then $\#E(F)[\mathrm{tors}]$ is bounded by a constant depending only on d. The best known bounds, due to J. Oesterlé (unpublished) and P. Parent [28], show that the prime powers appearing in the exponent of $E(F)[\mathrm{tors}]$ are bounded by quantities which are exponential d.

For certain classes of curves one can do much better. When the j-invariant of E is an algebraic integer, Hindry and Silverman [16] showed that for $d \geq 2$,

$$\#E(F)[\mathrm{tors}] \leq 1977408 d \log d.$$

Under the stronger assumption that E has complex multiplication (CM), it has recently been shown [7] that there is an effectively computable $C > 0$ such that

$$\forall d \geq 3,\ \ \#E(F)[\mathrm{tors}] \leq C d \log\log d. \tag{1}$$

Let $T_{\mathrm{CM}}(d)$ denote the largest size of a torsion subgroup of a CM elliptic curve defined over a number field of degree d. Combining (1) with work of Breuer [3] gives

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d\log\log d} \in (0,\infty). \tag{2}$$

In particular (1) is *sharp* up to the value of C.

Let $T(d)$ be the largest size of a torsion subgroup of an elliptic curve over a degree d number field, and let $T_{\neg\mathrm{CM}}(d)$ be the largest size of the torsion subgroup of an elliptic curve *without* complex multiplication over a degree d number field, so $T(d) = \max\{T_{\mathrm{CM}}(d),\ T_{\neg\mathrm{CM}}(d)\}$. We are far from knowing the truth about $T_{\mathrm{CM}}(d)$ but we expect — cf. [7, §1] — that $T_{\neg\mathrm{CM}}(d) = O(\sqrt{d\log\log d})$. Again Breuer's work provides lower bounds to show that such an upper bound would be sharp up to a constant. This would also imply that $T(d) = T_{\mathrm{CM}}(d)$ for infinitely many d.

It is not yet known whether $T(d) = T_{\mathrm{CM}}(d)$ for any $d \in \mathbb{Z}^+$. We have [24, 33]

$$T_{\mathrm{CM}}(1) = 6 < 16 = T(1),\ \ T_{\mathrm{CM}}(2) = 12 < 24 = T(2).$$

Since these are the only known values of $T(d)$, finding values of d for which $T(d) = T_{\mathrm{CM}}(d)$ seems beyond reach. But $T_{\mathrm{CM}}(d)$ is known for infinitely many values, so we can find values of d for which $T(d) > T_{\mathrm{CM}}(d)$. Especially, by [2, Theorem 1.4] we have

$$\text{For all primes } p \geq 7,\ T_{\mathrm{CM}}(p) = 6 < 16 = T(1) \leq T(p).$$

Moreover, from [6] we know $T_{\mathrm{CM}}(d)$ for all $d \leq 13$, which presents the prospect of showing $T(d) > T_{\mathrm{CM}}(d)$ for some further small values of d simply by exhibiting a non-CM elliptic curve in degree d with large enough torsion subgroup. We make use of the following recent computational results:

- Najman [26]: $T(3) \geq 21$.
- Jeon–Kim–Park [19]: $T(4) \geq 36$.
- van Hoeij [17]: $T(5) \geq 30$, $T(6) \geq 37$, $T(9) \geq 34$.

Combining with the calculations of [6] we find:

$$\forall d \in \{3, 4, 5, 6, 9\},\ T(d) > T_{\mathrm{CM}}(d).$$

On the other hand, we have $T_{\mathrm{CM}}(8) = T_{\mathrm{CM}}(10) = 50$, $T_{\mathrm{CM}}(12) = 84$, and there are no known non-CM elliptic curves with larger torsion subgroups in these degrees. In degree 8 the largest order of a torsion point on a CM elliptic curve is 39, whereas there is a point of order 50 on a non-CM elliptic curve in degree 8. However there is a point of order 50 on a CM elliptic curve of degree 10, and 50 is the largest value of N for which the tables in [17] record a degree 10 point on $Y_0(N)$. Further comparison of the tables of [17] to the work of [5] and [6] gives several values of N for which the smallest known degree of a point on $Y_1(N)$ is attained by a CM-point, e.g. $N \in \{57, 61, 67, 73, 79\}$.

In summary, it seems that the tools are not yet available to determine $T(d)$ for more than a few values of d, let alone to arrive at a theoretical understanding of the asymptotic behavior of this function. Henceforth we consider only the CM case, which is much more tractable and apparently related to the non-CM case in interesting ways.

1.2. **Anatomy of $T_{\mathrm{CM}}(d)$.** The goal of the present paper is to regard $T_{\mathrm{CM}}(d)$ as an "arithmetic function" and study its behavior for large values of d in the fashion that one studies functions like Euler's totient function φ. From this perspective, (2) gives the *upper order* of $T_{\mathrm{CM}}(d)$. However, as with more classical arithmetic functions, $T_{\mathrm{CM}}(d)$ exhibits considerable variation, and it is also interesting to ask about its lower order, its average order, and its "typical order" (roughly, its behavior away from a set of d of small density). It turns out that now is the right time to address these questions: by using — and, in some cases, sharpening — the results of [2] and [7], we find that we have enough information on the elliptic curve theory side to transport these questions into the realm of elementary/analytic number theory and then answer them.

We first determine the typical order (in a reasonable sense) of $T_{\mathrm{CM}}(d)$.

Theorem 1.1.

(i) *For all $\epsilon > 0$, there is a positive integer B_ϵ such that*

$$\overline{\delta}(\{d \in \mathbb{Z}^+ \mid T_{\mathrm{CM}}(d) \geq B_\epsilon\}) \leq \epsilon.$$

(ii) *For all $B \in \mathbb{Z}^+$, we have*

$$\underline{\delta}(\{d \in \mathbb{Z}^+ \mid T_{\mathrm{CM}}(d) \geq B\}) > 0.$$

Though stated separately for parallelism, the proof of Theorem 1.1(ii) is immediate. Indeed, starting with any CM elliptic curve $E/\mathbb{Q}$, we may adjoin the coordinates of a point of order N to obtain a field F_0 of degree d_0 (say). Considering extensions of F_0, we find that $T_{\mathrm{CM}}(d) \geq N$ whenever $d_0 \mid d$ and thus

$$\underline{\delta}(\{d \in \mathbb{Z}^+ \mid T_{\mathrm{CM}}(d) \geq B\}) \geq \frac{1}{d_0}.$$

We turn next to the average order of $T_{\mathrm{CM}}(d)$.

Theorem 1.2.

(i) *We have* $\frac{1}{x}\sum_{d\leq x} T_{\mathrm{CM}}(d) = x/(\log x)^{1+o(1)}$. *In other words: for all* $c < 1$,

$$\lim_{x\to\infty} \frac{\frac{1}{x}\sum_{d\leq x} T_{\mathrm{CM}}(d)}{x/\log^c x} = 0,$$

and for all $C > 1$ *we have*

$$\lim_{x\to\infty} \frac{\frac{1}{x}\sum_{d\leq x} T_{\mathrm{CM}}(d)}{x/\log^C x} = \infty.$$

(ii) *We have* $\frac{1}{x}\sum_{\substack{d\leq x\\ 2\nmid d}} T_{\mathrm{CM}}(d) = x^{1/3+o(1)}$. *In other words: for all* $c < \frac{1}{3}$,

$$\lim_{x\to\infty} \frac{\frac{1}{x}\sum_{\substack{d\leq x\\ 2\nmid d}} T_{\mathrm{CM}}(d)}{x^c} = \infty,$$

and for all $C > \frac{1}{3}$,

$$\lim_{x\to\infty} \frac{\frac{1}{x}\sum_{\substack{d\leq x\\ 2\nmid d}} T_{\mathrm{CM}}(d)}{x^C} = 0.$$

Remarks 1.1.

(i) The average order of $T_{\mathrm{CM}}(d)$ restricted to odd degrees is considerably smaller than its average order restricted to even degrees. This is another confirming instance of the odd/even dichotomy explored in [2].
(ii) The average order of $T_{\mathrm{CM}}(d)$ is considerably larger than the conjectural maximal order $\sqrt{d \log\log d}$ of $T(d)$.

Now we turn to the *lower order* of $T_{\mathrm{CM}}(d)$. When E is a CM elliptic curve over $\mathbb{Q}$, Olson [27] showed that there are precisely six possibilities for the group $E(\mathbb{Q})[\mathrm{tors}]$ (up to isomorphism): the trivial group $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We call these the *Olson groups*. From [2, Theorem 2.1(a)] we know that for any abelian variety defined over a number field $A_{/F}$ and all integers $d \geq 2$, there are infinitely many degree d extensions L/F with $A(L)[\mathrm{tors}] = A(F)[\mathrm{tors}]$. In particular, since the Olson groups occur over $\mathbb{Q}$, each of them occurs as the torsion subgroup of a CM elliptic curves over a number field of every degree, and thus $T_{\mathrm{CM}}(d) \geq 6$ for all d. Let us say that $d \in \mathbb{Z}^+$ is an *Olson degree* if the only torsion subgroups of CM elliptic curves in degree d are Olson groups. In [2, Theorem 1.4] it was shown that every prime number $d \geq 7$ is an Olson degree. We deduce

$$\liminf_{d\to\infty} T_{\mathrm{CM}}(d) = 6.$$

Remark 1.2. If d is an Olson degree, then $T_{\mathrm{CM}}(d) = 6$. In fact the converse holds, so the Olson degrees are precisely the degrees at which $T_{\mathrm{CM}}(d)$ attains its minimum value. This comes down to showing that if $T_{\mathrm{CM}}(d) = 6$, then there is no CM elliptic curve E defined over a degree d number field F with an F-rational point of order 5. But from [2, Theorem 1.5], the existence of such an $E_{/F}$ forces d to be even, and thus $T_{\mathrm{CM}}(d) \geq T_{\mathrm{CM}}(2) = 12$.

It is natural to ask for more precise information about the Olson degrees. Above we saw that the upper order of $T_{\mathrm{CM}}(d)$ is attained (or even approached) only on a very small set of d's. The result that all prime degrees $d \geq 7$ are Olson leaves open the possibility that the set of Olson degrees has density zero. In fact this is not the case.

Theorem 1.3. *The set of Olson degrees has positive asymptotic density.*

We also extend [2, Theorem 1.4] in the following complementary direction.

Theorem 1.4. *For all $n \in \mathbb{Z}^+$, there is a $P = P(n)$ such that for all primes $p \geq P$, the number p^n is an Olson degree.*

Finally we consider the distribution of groups G that realize the maximality of $T_{\mathrm{CM}}(d)$. Say that the finite abelian group G is a *maximal torsion subgroup in degree d* if $\#G = T_{\mathrm{CM}}(d)$ and there is a CM elliptic curve E over a degree d number field F with $E(F)[\mathrm{tors}] \cong G$. From the maximal order result in [7], each maximal torsion subgroup G in degree $d \leq x$ has size $O(x \log\log x)$. In view of Lemma 8.2 below, this leaves us with $\asymp x \log\log x$ possibilities for G. The next result describes how many such groups actually occur.

Theorem 1.5. *For $d \in \mathbb{Z}^+$, let $\mathcal{M}(d)$ be the set of isomorphism classes of groups G such that $\#G = T_{\mathrm{CM}}(d)$ and $G \cong E(F)$ for a CM elliptic curve E defined over a degree d number field F. Then*

$$\#\bigcup_{d \leq x} \mathcal{M}(d) = x/(\log x)^{1+o(1)}.$$

1.3. **Algebraic results.** In order to prove the results of the last section we need to sharpen and extend some of the algebraic results of [5] and [2].

The prototypical result that gives leverage on torsion in the CM case is the following theorem of Silverberg and Prasad-Yogananda [32, 30]: if $E_{/F}$ is an $\mathcal{O}$-CM elliptic curve defined over a number field F admitting an F-rational point of order N, then

$$\varphi(N) \leq \#\mathcal{O}^\times [F : \mathbb{Q}].$$

Moreover, if $F \supset K$ then

$$2\varphi(N) \leq \#\mathcal{O}^\times [F : \mathbb{Q}],$$

whereas if $F \not\supset K$ then

$$\varphi(\#E(F)[\mathrm{tors}]) \leq \#\mathcal{O}^\times [F : \mathbb{Q}].$$

We call these inequalities the *SPY bounds*. They were refined when N is prime in [5] and [2] by separate consideration of the cases in which N is split, inert or ramified in the CM field K. Moreover, at least in the case of CM by the maximal order, classical theory gives a tight relationship between F-rational torsion and the containment in F of ray class fields of K. The following result systematically relates SPY-type bounds, for prime powers N, to ray class containments.

N	# Olson degrees in $[1, N]$
1000	265
10,000	2649
100,000	26,474
1,000,000	264,633
10,000,000	2,646,355
100,000,000	26,462,845
1,000,000,000	264,625,698
10,000,000,000	2,646,246,218
100,000,000,000	26,462,418,808

TABLE 1. Counts of Olson degrees to 10^{11}.

Theorem 1.6. *Let F be a degree d number field containing an imaginary quadratic field K. Let $E_{/F}$ be an elliptic curve with $\mathcal{O}$-CM, where $\mathcal{O}$ is the order in K of discriminant Δ. Suppose $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, where $b \geq a \geq 0$ and $b \geq 1$. Then:*

(i) *If $\left(\frac{\Delta}{\ell}\right) = -1$, then $a = b$, and $\ell^{2b-2}(\ell^2 - 1) \mid w_K \cdot [F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$.*
(ii) *If $\left(\frac{\Delta}{\ell}\right) = 1$ and $a = 0$, then $\ell^{b-1}(\ell - 1) \mid w_K \cdot [F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$.*
(iii) *If $\left(\frac{\Delta}{\ell}\right) = 1$ and $a \geq 1$, then $\ell^{a+b-2}(\ell - 1)^2 \mid w_K \cdot [F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$.*
(iv) *If $\left(\frac{\Delta}{\ell}\right) = 0$ and ℓ ramifies in K, then $\ell^{a+b-1}(\ell - 1) \mid w_K \cdot [F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$.*
(v) *If $\left(\frac{\Delta}{\ell}\right) = 0$ and ℓ is unramified in K, then $\ell^{\max\{a+b-2,0\}}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right)) \mid w_K \cdot [F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$.*

These divisibility results combine in a natural way if one wants to consider the full group of F-rational torsion (see Theorem 2.4).

The other main algebraic result is a complete determination of all Olson degrees. Recall that a set of $\mathscr{A}$ of positive integers is called a *set of multiples* if whenever $a \in \mathscr{A}$, every multiple of $\mathscr{A}$ is also in $\mathscr{A}$. This is easily seen to be equivalent to requiring that $\mathscr{A} = M(\mathscr{G})$ for some set of positive integers $\mathscr{G}$, where

$$M(\mathscr{G}) = \{n \in \mathbb{Z}^+ : g \mid n \text{ for some } g \in \mathscr{G}\}.$$

We call $\mathscr{G}$ a set of *generators* for $\mathscr{A}$.

Theorem 1.7. *The set of non-Olson degrees can be written as $M(\mathscr{G})$, where*

$$\mathscr{G} = \{2\} \cup \left\{ \frac{\ell - 1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \mid \ell \equiv 3 \pmod 4,\ \ell > 3 \right\}.$$

An algorithm for computing all torsion subgroups of CM elliptic curves in degree d is presented in [6]. In principle this algorithm allows us to determine whether a given degree d is Olson. However, the algorithm requires as input the list of all imaginary quadratic fields of class number properly dividing d so is for sufficiently large composite d quite impractical. In contrast, using Theorem 1.7, one can compute in a day on a modern desktop computer that there are 26,462,418,808 Olson degrees $d \leq 10^{11}$. Since $\pi(10^{11}) = 4{,}118{,}054{,}813$, this adds 22,344,363,994 composite values of d for which the complete list of torsion subgroups of CM elliptic curves in degree d is known. Such calculations suggest that the density of Olson degrees, which by Theorem 1.3 lies in $(0, 1)$, is in fact slightly larger than $\frac{1}{4}$; see Table 1.

We also found that for all primes $p > 5$ and all $n \in \mathbb{Z}^+$, if $p^n \leq 10^{30}$ then p^n is an Olson degree.[1] Thus we conjecture the following strengthening of Theorem 1.4.

Conjecture 1.8. *p^n is an Olson degree for every prime $p > 5$ and all $n \in \mathbb{Z}^+$.*

2. Divisibility requirements for rational torsion

The next two results are taken from the already mentioned work [7].

Lemma 2.1 ([7, Theorem 5])**.** *Let K be an imaginary quadratic field, $F \supset K$ be a number field, $E_{/F}$ a K-CM elliptic curve, and $N \in \mathbb{Z}^+$. If $(\mathbb{Z}/N\mathbb{Z})^2 \hookrightarrow E(F)$, then $F \supset K^{(N\mathcal{O}_K)}$.*

Lemma 2.2 ([7, Theorem 6])**.** *Let K be an imaginary quadratic field, $F \supset K$ a number field, and $E_{/F}$ an $\mathcal{O}$-CM elliptic curve. Suppose that $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, where $b \geq a \geq 0$ and $b \geq 1$. Then $[F(E[\ell^b]) : F] \leq \ell^{b-a}$. In fact, letting Δ denote the discriminant of $\mathcal{O}$, we have the following more precise results:*

(i) *If $\left(\frac{\Delta}{\ell}\right) = 0$ or $= -1$, then $[F(E[\ell^b]) : F] \mid \ell^{b-a}$.*
(ii) *If $\left(\frac{\Delta}{\ell}\right) = 1$, then either $a = 0$ and $[F(E[\ell^b]) : F] \mid (\ell - 1)\ell^{b-1}$, or $a > 0$ and $[F(E[\ell^b]) : F] \mid \ell^{b-a}$.*

Remark 2.1. Statements (i) and (ii) are not explicitly included in [7, Theorem 6]; however, they follow immediately from the proof. In fact, as we recall below, when $\left(\frac{\Delta}{\ell}\right) = -1$ we always have $b = a$.

Lemma 2.3. *Let F be a degree d number field containing an imaginary quadratic field K. Let $E_{/F}$ be an elliptic curve with $\mathcal{O}$-CM, where $\mathcal{O}$ is the order in K of discriminant Δ. Suppose $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, where $b \geq a \geq 0$ and $b \geq 1$. If*

(i) *$\left(\frac{\Delta}{\ell}\right) = -1$, then $a = b$, and $h_K \cdot \ell^{2b-2}(\ell^2 - 1) \mid w_K \frac{d}{2}$,*
(ii) *$\left(\frac{\Delta}{\ell}\right) = 1$ and $a = 0$, then $h_K \cdot \ell^{b-1}(\ell - 1) \mid w_K \frac{d}{2}$,*
(iii) *$\left(\frac{\Delta}{\ell}\right) = 1$ and $a > 0$, then $h_K \cdot \ell^{a+b-2}(\ell - 1)^2 \mid w_K \frac{d}{2}$,*
(iv) *$\left(\frac{\Delta}{\ell}\right) = 0$ and ℓ ramifies in K, then $h_K \cdot \ell^{a+b-1}(\ell - 1) \mid w_K \frac{d}{2}$,*
(v) *$\left(\frac{\Delta}{\ell}\right) = 0$ and ℓ is unramified in K, then $h_K \cdot \ell^{\max\{a+b-2,0\}}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right)) \mid w_K \frac{d}{2}$.*

Proof. We follow the proof of [2, Theorem 4.6]. By Lemma 2.1, $K^{(\ell^b\mathcal{O}_K)} \subset F(E[\ell^b])$. Recalling that $K(j(E))$ is a ring class field of K, we see that $F \supset K(j(E)) \supset K^{(\mathcal{O}_K)}$. Let $d_0 = [F(E[\ell^b]) : F]$.

The Hilbert class field $K^{(\mathcal{O}_K)}$ has degree h_K over K. From [4, Proposition 2.1, p. 50], the degree of $K^{(\ell^b\mathcal{O}_K)}$ over $K^{(\mathcal{O}_K)}$ is $\frac{\Phi(\ell^b)}{[U:U_{\ell^b}]}$. Here Φ is the analogue of Euler's function for the ideals of $\mathcal{O}_K$, so that

$$\Phi(\ell^b) = \#(\mathcal{O}_K/\ell^b\mathcal{O}_K)^\times = \ell^{2b-2}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right)),$$

[1] A warning: To perform the above computations, we made extensive use of the `PARI/GP` command `quadclassunit` to compute class numbers of imaginary quadratic fields. That algorithm has been proved correct *only under the assumption of the Generalized Riemann Hypothesis*. However, the counts up to 10^6 in Table 1 have been certified unconditionally, as has the result that there are no non-Olson prime powers $p^n \leq 10^{14}$ (with $p > 5$).

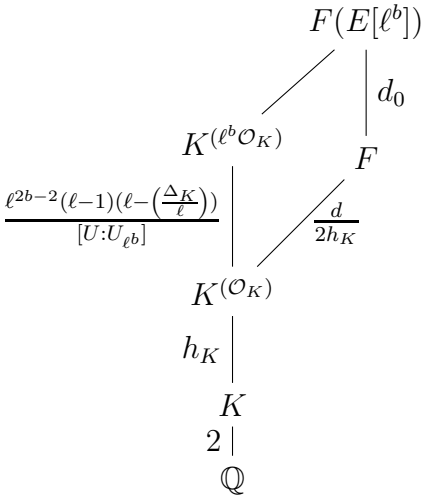

FIGURE 1. Diagram of fields appearing in the proof of Lemma 2.3.

$U = \mathcal{O}_K^\times$, and U_{ℓ^b} is the subgroup of units congruent to 1 (mod ℓ^b). Since $[U : U_{\ell^b}]$ divides w_K,

$$\ell^{2b-2}(\ell-1)(\ell-\left(\frac{\Delta_K}{\ell}\right)) \mid w_K \cdot [F(E[\ell^b]) : K^{(\mathcal{O}_K)}] = w_K \frac{d}{2h_K} d_0.$$

Thus,

$$\frac{\ell^{2b-2}(\ell-1)(\ell-\left(\frac{\Delta_K}{\ell}\right))}{\gcd(\ell^{2b-2}(\ell-1)(\ell-\left(\frac{\Delta_K}{\ell}\right)), d_0)} \mid w_K \frac{d}{2h_K}. \tag{3}$$

Suppose that $\left(\frac{\Delta}{\ell}\right) = -1$. In this case, the existence of a single F-rational point of order ℓ^b implies that $E(F)$ contains $E[\ell^b]$. Indeed, as shown in the proof of [2, Theorem 4.8], any torsion point of order ℓ^b generates $E[\ell^b]$ as an $\mathcal{O}$-module. Thus, $a = b$ and $d_0 = 1$, and we obtain the first possibility in the lemma statement.

Suppose next that $\left(\frac{\Delta}{\ell}\right) = 1$ and $a = 0$. Lemma 2.2 shows that $d_0 \mid \ell^{b-1}(\ell-1)$, so that the left-hand side of (3) is divisible by $\ell^{b-1}(\ell-1)$. Thus, we have the second possibility indicated in the lemma. If $\left(\frac{\Delta}{\ell}\right) = 1$ and $a > 0$, then $d_0 \mid \ell^{b-a}$, and the left-hand side of (3) is divisible by $\ell^{a+b-2}(\ell-1)^2$. This gives the third possibility indicated in the lemma statement.

Finally, suppose that $\left(\frac{\Delta}{\ell}\right) = 0$. If ℓ ramifies in K, we use that $d_0 \mid \ell^{b-a}$ to deduce that the left-hand side of (3) is divisible by $\ell^{a+b-1}(\ell-1)$. If ℓ is unramified in K, we use that the denominator in (3) divides $\ell^{\min\{b-a,2b-2\}}$ to deduce that the left-hand side of (3) is divisible by $\ell^{\max\{a+b-2,0\}}(\ell-1)(\ell-\left(\frac{\Delta_K}{\ell}\right))$. In this way, we obtain the fourth and fifth possibilities in the lemma statement. □

Proof of Theorem 1.6. Note that $[FK^{(\ell^b\mathcal{O}_K)} : F] = [K^{(\ell^b\mathcal{O}_K)} : F \cap K^{(\ell^b\mathcal{O}_K)}]$, and that this common value divides both $[F(E[\ell^b]) : F] = d_0$ and $[K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}] = \Phi(\ell^b)/[U : U_{\ell^b}]$. Consequently, $[K^{(\ell^b\mathcal{O}_K)} : F \cap K^{(\ell^b\mathcal{O}_K)}] \mid \gcd(\Phi(\ell^b), d_0)$, and so

$$[K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}] \mid \gcd(\Phi(\ell^b), d_0) \cdot [F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}].$$

Multiply through by $[U : U_{\ell^b}]$ to find that

$$\frac{\Phi(\ell^b)}{\gcd(\Phi(\ell^b), d_0)} \mid [U : U_{\ell^b}] \cdot [F \cap K^{(\ell^b \mathcal{O}_K)} : K^{(\mathcal{O}_K)}] \mid w_K \cdot [F \cap K^{(\ell^b \mathcal{O}_K)} : K^{(\mathcal{O}_K)}].$$

But the first term on the left coincides with the left-hand side of (3). The theorem now follows from the case-by-case analysis found in the proof of Lemma 2.3. □

Thus far we have examined the divisibility requirements for rational torsion prime-by-prime. However, the conditions combine in a natural way to give divisibility results for the full group of rational torsion. Let F be a number field containing an imaginary quadratic field K, and let $E_{/F}$ be an elliptic curve with CM by an order in K of discriminant Δ. Suppose $\#E(F)[\text{tors}] = n$. For each $\ell \mid n$, we have $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^{a_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{b_\ell}\mathbb{Z}$, where $b_\ell \geq a_\ell \geq 0$ and $b_\ell \geq 1$. Thus, $\ell^{\alpha_\ell} \parallel n$, where $\alpha_\ell := a_\ell + b_\ell$. For each ℓ^{α_ℓ}, we define a constant $\lambda_{\ell^{\alpha_\ell}}$ in the following way:

(i) If $\left(\frac{\Delta}{\ell}\right) = -1$, then $\lambda_{\ell^{\alpha_\ell}} := \ell^{2b_\ell - 2}(\ell^2 - 1)$.
(ii) If $\left(\frac{\Delta}{\ell}\right) = 1$ and $a_\ell = 0$, then $\lambda_{\ell^{\alpha_\ell}} := \ell^{b_\ell - 1}(\ell - 1)$.
(iii) If $\left(\frac{\Delta}{\ell}\right) = 1$ and $a_\ell \geq 1$, then $\lambda_{\ell^{\alpha_\ell}} := \ell^{a_\ell + b_\ell - 2}(\ell - 1)^2$.
(iv) If $\left(\frac{\Delta}{\ell}\right) = 0$ and ℓ ramifies in K, then $\lambda_{\ell^{\alpha_\ell}} := \ell^{a_\ell + b_\ell - 1}(\ell - 1)$.
(v) If $\left(\frac{\Delta}{\ell}\right) = 0$ and ℓ is unramified in K, then $\lambda_{\ell^{\alpha_\ell}} := \ell^{\max\{a_\ell + b_\ell - 2, 0\}}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right))$.

Note that by Theorem 1.6, we have $\lambda_{\ell^{\alpha_\ell}} \mid w_K \cdot [F \cap K^{(\ell^{b_\ell} \mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$.

Theorem 2.4. *Suppose that there is a K-CM elliptic curve E over a degree d number field $F \supset K$ with $\#E(F)[\text{tors}] = n$. Then $h_K \cdot \prod_{\ell \mid n} \lambda_{\ell^{\alpha_\ell}} \mid 6d$.*

Proof. Take any K-CM elliptic curve $E_{/F}$ with $[F : \mathbb{Q}] = d$ and $\#E(F)[\text{tors}] = n$. Let $\mathcal{O}$ be the CM order, and say Δ is the discriminant of $\mathcal{O}$. As above, for each $\ell \mid n$, write $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^{a_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{b_\ell}\mathbb{Z}$, where $b_\ell \geq a_\ell \geq 0$ and $b_\ell \geq 1$. Let N be the exponent of $E(F)[\text{tors}]$, so that $N = \prod_{\ell \mid n} \ell^{b_\ell}$. Let $d_{0,\ell}$ denote the degree $[F(E[\ell^{b_\ell}]) : F]$, and observe that the degree d_0 of $F(E[N])/F$ satisfies

$$d_0 \mid \prod_{\ell \mid n} d_{0,\ell}.$$

Using that $F(E[N]) \supset K^{(N\mathcal{O}_K)}$, we find that

(4)
$$\prod_{\ell \mid n} \ell^{2b_\ell - 2}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right)) = [U : U_N] \cdot [K^{(N\mathcal{O}_K)} : K^{(\mathcal{O}_K)}] \mid w_K \frac{d}{2h_K} d_0 \mid w_K \frac{d}{2h_K} \prod_{\ell \mid n} d_{0,\ell}.$$

Suppose first that $\alpha_\ell := a_\ell + b_\ell \geq 2$. Then the case analysis in the proof of Lemma 2.3 shows that $d_{0,\ell} \mid \ell^{2b_\ell - 2}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right))$, and that the quotient $\ell^{2b_\ell - 2}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right))/d_{0,\ell}$ is a multiple of $\lambda_{\ell^{\alpha_\ell}}$.

Now suppose that $\alpha_\ell = 1$. Then $a_\ell = 0$ and $b_\ell = 1$. Note that we cannot have $\left(\frac{\Delta}{\ell}\right) = -1$ in this case, since that condition forces $a_\ell = b_\ell$. If $\left(\frac{\Delta}{\ell}\right) = 1$, then $d_{0,\ell} \mid \ell - 1$, and so

$$\lambda_\ell = \ell - 1 \mid \ell^{2b_\ell - 2}(\ell - 1)(\ell - \left(\frac{\Delta_K}{\ell}\right))/d_{0,\ell}. \tag{5}$$

If $\left(\frac{\Delta}{\ell}\right) = 0$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$, then $d_{0,\ell} \mid \ell$, so that again (5) holds. Note that if $\left(\frac{\Delta}{\ell}\right) = 0$ but $\left(\frac{\Delta_K}{\ell}\right) \neq 0$, then $d_{0,\ell} \mid \ell$ while

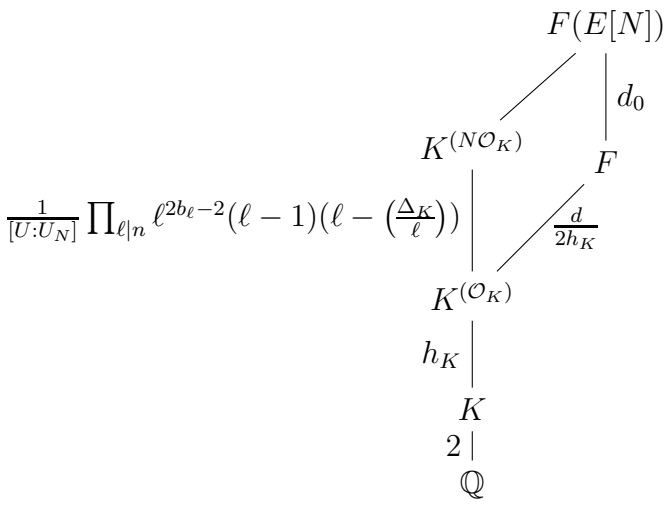

FIGURE 2. Diagram of fields appearing in the proof of Theorem 2.4.

$$\lambda_\ell = \ell^{2b_\ell-2}(\ell-1)(\ell-\left(\frac{\Delta_K}{\ell}\right)) \in \{\ell^2-1, (\ell-1)^2\}.$$

Let $\mathscr{S}_1$ be the set of prime powers ℓ^{α_ℓ} exactly dividing n for which either $\alpha_\ell \geq 2$, or $\alpha_\ell = 1$ and either $\left(\frac{\Delta}{\ell}\right) \neq 0$ or $\left(\frac{\Delta_K}{\ell}\right) = 0$. Let $\mathscr{S}_2$ be the complementary set of exact prime powers divisors of n. Of course, $\mathscr{S}_2$ actually consists only of primes. Referring back to (4),

$$\prod_{\ell^{\alpha_\ell}\in\mathscr{S}_1} \lambda_{\ell^{\alpha_\ell}} \prod_{\ell\in\mathscr{S}_2} \lambda_\ell \mid w_K \frac{d}{2h_K} \prod_{\ell\in\mathscr{S}_2} \ell. \tag{6}$$

On the other hand, Theorem 1.6 implies

$$\lambda_{\ell^{\alpha_\ell}} \mid w_K \cdot [F \cap K^{(\ell^{b_\ell}\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$$

for each prime ℓ dividing n. The fields $F \cap K^{(\ell^{b_\ell}\mathcal{O}_K)}$ are linearly disjoint extensions of $K^{(\mathcal{O}_K)}$, all contained in F. Thus, with $m \coloneqq \omega(n)$,

$$\prod_{\ell^{\alpha_\ell}\in\mathscr{S}_1} \lambda_{\ell^{\alpha_\ell}} \prod_{\ell\in\mathscr{S}_2} \lambda_\ell \mid w_K^m \cdot [F : K^{(\mathcal{O}_K)}] = w_K^m \cdot \frac{d}{2h_K}. \tag{7}$$

Putting (6) and (7) together, we find

$$\prod_{\ell^{\alpha_\ell}\in\mathscr{S}_1} \lambda_{\ell^{\alpha_\ell}} \prod_{\ell\in\mathscr{S}_2} \lambda_\ell \mid w_K \frac{d}{2h_K} \prod_{\ell\in\mathscr{S}_2,\, \ell|w_K} \ell. \tag{8}$$

If $w_K = 2$, it follows that

$$\prod_{\ell^{\alpha_\ell}\in\mathscr{S}_1} \lambda_{\ell^{\alpha_\ell}} \prod_{\ell\in\mathscr{S}_2} \lambda_\ell \mid 2\frac{d}{h_K}.$$

In fact, if $w_K = 4$, the same divisibility condition holds. Indeed, 2 is the only prime that divides w_K, but $2 \notin \mathscr{S}_2$ since 2 ramifies in $K = \mathbb{Q}(i)$. If $w_K = 6$, then $3 \notin \mathscr{S}_2$

since 3 ramifies in $K = \mathbb{Q}(\sqrt{-3})$, and (8) implies

$$\prod_{\ell^{\alpha_\ell} \in \mathscr{S}_1} \lambda_{\ell^{\alpha_\ell}} \prod_{\ell \in \mathscr{S}_2} \lambda_\ell \mid 6\frac{d}{h_K}. \qquad \square$$

As a consequence, in the case of $\mathcal{O}_K$-CM elliptic curves, we recover the SPY Bounds as divisibilities.

Corollary 2.5 (SPY Divisibilities)**.** *Let F be a number field of degree d containing an imaginary quadratic field K, and let $E_{/F}$ be an $\mathcal{O}_K$-CM elliptic curve. If E has an F-rational point of order N, then*

$$h_K \varphi(N) \mid \frac{w_K}{2} \cdot d.$$

Proof. Suppose $E_{/F}$ has a point of order $N = \prod \ell^{e_\ell}$. For each $\ell \mid N$,

$$E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^{a_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{b_\ell}\mathbb{Z},$$

where $b_\ell \geq a_\ell \geq 0$ and $b_\ell \geq e_\ell$. Since E has CM by the maximal order, there are no primes of type $\mathscr{S}_2$, and for each $\ell^{\alpha_\ell} \in \mathscr{S}_1$ we have $\varphi(\ell^{b_\ell}) \mid \lambda_{\ell^{\alpha_\ell}}$. Thus by (6) we have

$$\varphi(N) = \prod_{\ell \mid N} \varphi(\ell^{e_\ell}) \mid \prod_{\ell \mid N} \varphi(\ell^{b_\ell}) \mid \prod_{\ell^{\alpha_\ell} \in \mathscr{S}_1} \lambda_{\ell^{\alpha_\ell}} \mid w_K \frac{d}{2h_K}. \qquad \square$$

Remarks 2.2. Let us discuss the sharpness of the divisibilities obtained in Theorem 1.6.

(a) If $\ell \neq 2$ and $a = b$, then in every case Theorem 1.6 gives

$$\ell^{2b-2}(\ell-1)(\ell - \left(\frac{\Delta_K}{\ell}\right))/w_K \mid [K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}].$$

Since in fact we have

$$[K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}] = \ell^{2b-2}(\ell-1)(\ell - \left(\frac{\Delta_K}{\ell}\right))/w_K,$$

Theorem 1.6 is sharp in this case, which includes all of Case (i).

(b) If $\left(\frac{\Delta}{\ell}\right) = 1$ and $a = 0$, the image of the ℓ-adic Galois representation lands in a split Cartan subgroup (cf. [2, §3.4]). Thus for all $n \in \mathbb{Z}^+$ we have an F-rational subgroup of order ℓ^n. If ℓ is an odd prime, it follows from [2, Theorem 7.2] that there is an $\mathcal{O}_K$-CM elliptic curve E defined over an extension $L/K^{(\mathcal{O}_K)}$ with $[L : K^{(\mathcal{O}_K)}] = \varphi(\ell^n)/2$ such that $E(L)$ contains a point of order ℓ^n. Thus the divisibility condition given is best possible when $w_K = 2$ and ℓ is odd.

(c) In Theorem 1.6 we recorded the divisibilities in terms of $[F \cap K^{(\ell^b\mathcal{O}_K)} : K^{(\mathcal{O}_K)}]$ rather than in terms of $[F : K] = [F : K^{(\mathcal{O}_K)}]h_K$ because we get a stronger result by doing so. However, it may be more natural to ask for best possible divisibilities of $[F : K]$. In part (b) above, the optimality occurs in this stronger sense. As for part (a), when ℓ does not divide the conductor $\mathfrak{f}$ of the order $\mathcal{O}$, classical CM theory implies that there is an elliptic curve defined over $K^{(\ell^b)}$ with full ℓ^b-torsion and thus multiplying the bound of Theorem 1.6 by h_K gives the optimal divisibility of $[F : K]$ in this case.

(d) The field F also contains the ring class field $K(\mathcal{O})$ of the order $\mathcal{O}$. Let $\mathfrak{f}_\ell = \mathrm{ord}_\ell(\mathfrak{f}(\mathcal{O}))$ and suppose that $\mathfrak{f}_\ell \geq 1$. (This is the condition under which we cannot reduce to the case of $\mathcal{O}_K$-CM.) For all $\ell > 2$ we have

$$\mathrm{ord}_\ell[K(\mathcal{O}) : K^{(\mathcal{O}_K)}] = \ell^{\mathfrak{f}_\ell - 1},$$

so if $\mathfrak{f}_\ell > 2b - |\left(\frac{\Delta_K}{\ell}\right)|$ then there is a larger power of ℓ dividing $[F : K^{(\mathcal{O}_K)}]$ than is given by Theorem 1.6. (This does not say that Theorem 1.6 is not optimal but rather that it could be refined by considering an additional parameter.)

(e) In case (v) of Theorem 1.6, there are values of a and b for which we suspect that the divisibility on $d = [F : K]$, at least, can be improved. Suppose $w_K = 2$, $b = 2$, $a = 0$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$. In this case Theorem 1.6 implies $h_K(\ell - 1)^2 \mid d$, whereas the SPY bounds here give $\ell(\ell - 1) \leq d$: this is not quite implied by our result! In light of Corollary 2.5 it is reasonable to expect in all cases the SPY bounds may be multiplied by a factor of h_K and yield divisibilities.[2] If so, the two results would combine to give $h_K\ell(\ell - 1)^2 \mid d$. Note that by part (d) this certainly occurs if $\mathfrak{f}_\ell \geq 2$, so the open case is precisely $\mathfrak{f}_\ell = 1$.

3. Proof of Theorem 1.1: Typical boundedness of $T_{\mathrm{CM}}(d)$

We need a result from the part of number theory known as the 'anatomy of integers'.

Proposition 3.1 (Erdős–Wagstaff [10, Theorem 2])**.** *For all $\epsilon > 0$, there is a positive integer B'_ϵ such that the set of positive integers which are divisible by $\ell - 1$ for some prime $\ell > B'_\epsilon$ has upper density at most ϵ.*

Proof of Theorem 1.1. Suppose that

$$T_{\mathrm{CM}}(d) > B. \tag{9}$$

We will see that if B is a constant chosen sufficiently large in terms of ϵ, then for large x the inequality (9) has fewer than ϵx solutions $d \leq x$.

Choose a degree d number field F and a CM elliptic curve $E_{/F}$ with $\#E(F)[\mathrm{tors}] > B$. Let K denote the CM field. Suppose to start with that $\#E(F)[\mathrm{tors}]$ has a prime factor $\ell > B' + 1$, where $B' = B'_{\epsilon/24}$, in the notation of Proposition 3.1. Since ℓ divides $\#E'(FK)[\mathrm{tors}]$, Lemma 2.3 shows that

$$\ell - 1 \mid w_K \frac{[FK : \mathbb{Q}]}{2} \mid w_K d \mid 12d.$$

Note that $12d \leq 12x$. By the definition of B', once x is large, there are fewer than $\frac{\epsilon}{24} \cdot 12x = \frac{\epsilon}{2}x$ possibilities for $12d$, and so also at most $\frac{\epsilon}{2}x$ possibilities for d.

Now suppose instead that each prime factor of $\#E(F)[\mathrm{tors}]$ is at most $B' + 1$. Then $\#E(F)[\mathrm{tors}]$ has at most $r := \pi(B' + 1)$ distinct prime factors, and so we can choose a prime power $\ell^\alpha \parallel \#E(F)[\mathrm{tors}]$ with

$$\ell^\alpha \geq (\#E(F)[\mathrm{tors}])^{1/r} > B^{1/r}.$$

Let us impose the restriction that $B \geq (B' + 1)^r$. Then $\ell^\alpha > B' + 1 \geq \ell$, and so $\alpha \geq 2$. Applying Lemma 2.3 in the same manner as above, we find that $12d$ is divisible by either $\ell^{\alpha-2}(\ell^2 - 1)$, $\ell^{\alpha-1}(\ell - 1)$, or $\ell^{\alpha-2}(\ell - 1)^2$. Thus, the number of possibilities for $12d$ is bounded by

$$12x\left(\frac{1}{\ell^{\alpha-2}(\ell^2-1)} + \frac{1}{\ell^{\alpha-1}(\ell-1)} + \frac{1}{\ell^{\alpha-2}(\ell-1)^2}\right) \leq 12x\left(\frac{4/3}{\ell^\alpha} + \frac{2}{\ell^\alpha} + \frac{4}{\ell^\alpha}\right) < 100\frac{x}{\ell^\alpha}.$$

[2] In fact, we believe that Silverberg's arguments can be easily adapted to yield these strengthenings. We will revisit this in a later work.

Now sum on the possible values of ℓ^α. We find that the number of choices for d is at most

$$100x \sum_{\substack{\ell^\alpha > B^{1/r} \\ \ell \le B'+1 \\ \alpha \ge 2}} \frac{1}{\ell^\alpha} = 100x \sum_{\ell \le B'+1} \sum_{\substack{\alpha:\, \alpha \ge 2 \\ \ell^\alpha > B^{1/r}}} \frac{1}{\ell^\alpha}.$$

The geometric series appearing as the inner sum is at most twice its largest term; this yields an upper bound for the right-hand side of $\frac{200r}{B^{1/r}}x$. Now impose the additional restriction that $B > (\frac{400r}{\epsilon})^r$. Then our upper bound here is smaller than $\frac{\epsilon}{2}x$. Putting this together with the result of the last paragraph finishes the proof. □

Remark 3.1. By a more refined analysis, using techniques recently developed to study the range of Carmichael's λ-function [23, 11], one can establish the following sharpening of Theorem 1.1: as $B \to \infty$, the upper and lower densities of $\{n \mid T_{\mathrm{CM}}(d) > B\}$ both take the form $(\log B)^{-\eta+o(1)}$. Here

$$\eta = 1 - \frac{1 + \log\log 2}{\log 2} = 0.08607\ldots,$$

the *Erdős–Ford–Tenenbaum constant*. Details will be presented elsewhere.

4. Proof of Theorem 1.7: Characterization of Olson degrees

As already mentioned in the introduction, any group that appears as the torsion subgroup of a CM elliptic curve over a degree d number field also appears over some degree d' number field, for each multiple d' of d (see [2, Theorem 2.1(a)]). So the set of non-Olson degrees is indeed a set of multiples.

To prove that the set $\mathscr{G}$ appearing in the statement of Theorem 1.7 is a set of generators, we need the following results from [2].

Proposition 4.1 ([2, Theorem 4.9])**.** *Let F be a number field that admits a real embedding, and let $E_{/F}$ be a K-CM elliptic curve. If $E(F)$ contains a point of order n, then $\mathbb{Q}(\zeta_n) \subset FK$.*

Proposition 4.2 ([2, Theorem 7.1])**.** *Let F be a number field of odd degree, and let $E_{/F}$ be a CM elliptic curve. Then $E(F)[\mathrm{tors}]$ is isomorphic to one of the following groups:*

(i) *the trivial group $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,*
(ii) *the group $\mathbb{Z}/\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \pmod 8$ and some positive integer n,*
(iii) *the group $\mathbb{Z}/2\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \pmod 4$ and some positive integer n.*

Conversely, each of these groups appears as the torsion subgroup of some CM elliptic curve over some odd degree number field.

Proposition 4.3 ([2, Corollary 7.5])**.** *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant Δ, and let $\ell > 2$ be a prime dividing Δ. There is a number field L of degree $\frac{\ell-1}{2} \cdot h(\mathcal{O})$ and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ with an L-rational point of order ℓ.*

Proof of Theorem 1.7. First we verify that any $d \in \mathscr{G}$ is non-Olson. By [2, Theorem 1.4], 2 is a non-Olson degree. It remains to consider $d = \frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})}$ for a prime $\ell > 3$ with $\ell \equiv 3 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{-\ell})$. By Proposition 4.3, there is an $\mathcal{O}_K$-CM elliptic

curve E defined over a number field L of degree $\frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})}$ such that $E(L)$ contains a point of order ℓ. Thus $E(L)[\text{tors}]$ is not an Olson group and d is a non-Olson degree.

Next, we suppose d is a non-Olson degree and show $d \in M(\mathscr{G})$. There is an elliptic curve E defined over a number field F of degree d for which $E(F)[\text{tors}]$ is not an Olson group. Since $2 \in \mathscr{G}$, we may assume that d is odd and hence that F admits a real embedding.

By Proposition 4.2, $E(F)$ contains a point of prime order ℓ where $\ell \equiv 3 \pmod 4$. By Proposition 4.1, $\mathbb{Q}(\zeta_\ell) \subset FK$, where K is the CM field. Thus, FK contains the quadratic subfield $\mathbb{Q}(\sqrt{-\ell})$ of $\mathbb{Q}(\zeta_\ell)$. Since $4 \nmid [FK : \mathbb{Q}]$, the field FK can contain only one quadratic subfield, and so $K = \mathbb{Q}(\sqrt{-\ell})$.

Suppose first that $\ell > 3$. Then Lemma 2.3 shows that $h_K \cdot (\ell-1) \mid w_K \frac{[FK:\mathbb{Q}]}{2} = 2d$. Thus $h_K \cdot \frac{\ell-1}{2} \mid d$ and $d \in M(\mathscr{G})$. Now suppose $\ell = 3$. Since $E(F)[\text{tors}]$ is not Olson, it must have a point of order 9. By Proposition 4.1, $\mathbb{Q}(\zeta_9) \subset FK$. Thus $6 \mid [FK : \mathbb{Q}] = 2d$, so $3 \mid d$. But $3 = \frac{7-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-7})}$, so again $d \in M(\mathscr{G})$. □

5. Proof of Theorem 1.3: Olson degrees have positive density

Theorem 1.3 follows from Theorem 1.7 together with the following elementary result from the theory of sets of multiples.

Lemma 5.1. *Let $\mathscr{G} \subset \mathbb{Z}^+$. If $\sum_{g \in \mathscr{G}} \frac{1}{g} < \infty$, then $M(\mathscr{G})$ has an asymptotic density. If moreover $1 \notin \mathscr{G}$, then the density of $M(\mathscr{G})$ is strictly less than 1.*

Proof. See Theorem 0.1 and Corollary 0.10 in Chapter 0 of Hall's monograph [12]. □

We can now prove Theorem 1.3.

Proof of Theorem 1.3. In view of Lemma 5.1, it suffices to show that $\sum_{g \in \mathscr{G}} \frac{1}{g} < \infty$, where $\mathscr{G}$ is the set defined in Theorem 1.7. Siegel's theorem (see for instance [18, p. 124]) implies that for each $\epsilon > 0$,

$$\frac{\ell - 1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \gg_\epsilon \ell^{3/2-\epsilon}.$$

Fixing any $\epsilon < \frac{1}{2}$, we obtain the desired convergence. Alternatively, the work of Goldfeld–Gross–Zagier yields an effective lower bound $\frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \gg_\epsilon \ell (\log \ell)^{1-\epsilon}$ (see [18, p. 540]). Now fixing $\epsilon \in (0, 1)$, partial summation along with the prime number theorem gives that $\sum_\ell \frac{1}{\ell (\log \ell)^{1-\epsilon}} < \infty$. □

Remark 5.1. By another appeal to Proposition 3.1, one can prove Theorem 1.3 without using any lower bounds on $h_{\mathbb{Q}(\sqrt{-\ell})}$. Compare with the proof of [29, Theorem 4].

6. Proof of Theorem 1.4: Prime power Olson degrees

Proof of Theorem 1.4. If $p \leq 5$, then p and its powers are non-Olson degrees, so we assume that $p \geq 7$. Suppose that p^n is not an Olson degree. From the classification of Olson degrees (Theorem 1.7), there is a prime $\ell > 3$ with $\ell \equiv 3 \pmod 4$ for which $\frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \mid p^n$. Hence, there are integers $r \geq 1$ and $s \geq 0$ with $r + s \leq n$,

$$\frac{\ell - 1}{2} = p^r, \quad \text{and} \quad h_{\mathbb{Q}(\sqrt{-\ell})} = p^s.$$

We argue that p is bounded (ineffectively) in terms of n. By Siegel's theorem, if p is large in terms of n, then $h_{\mathbb{Q}(\sqrt{-\ell})} > \ell^{\frac{1}{2}-\frac{1}{3n}} > p^{\frac{r}{2}-\frac{1}{3}}$. Using the elementary explicit upper bound

$$h_{\mathbb{Q}(\sqrt{-\ell})} \leq \ell^{1/2} \log \ell, \tag{10}$$

(see, e.g., [20, §2]) we find that for p large enough in terms of n, we also have $h_{\mathbb{Q}(\sqrt{-\ell})} < p^{\frac{r}{2}+\frac{1}{3}}$. Thus, $p^{-1/3} < p^{s-\frac{r}{2}} < p^{1/3}$. Since $s - r/2$ is an integer or half-integer, we must have $s = r/2$. In particular, $r = 2s$ is even. But then $\ell = 2p^{2s} + 1 \equiv 0 \pmod 3$, contradicting that $\ell > 3$. □

Remark 6.1. For general n, the ineffectivity of Siegel's theorem prevents us from giving a concrete bound on the largest non-Olson prime power p^n. However, as we explain below, the above argument can be made effective when $n = 1, 2$, or 3. In this way, we obtain a simple proof that p^n is Olson for every $p > 5$. (Recall that when $n = 1$, this was proved already in [2].)

Given a counterexample, choose ℓ, r, and s as in the above proof. As before, working modulo 3 shows that r is odd. To finish the proof, it suffices to prove that $s = 0$, i.e., $h_{\mathbb{Q}(\sqrt{-\ell})} = 1$. To see that this is enough, notice that $\ell = 2p+1$ or $2p^3+1$, where $p > 5$, so that $\ell > 11$. Now if K is an imaginary quadratic field with $h_K = 1$, an elementary argument shows that every prime smaller than $\frac{1+|\Delta_K|}{4}$ is inert in K. In particular, 3 is inert in $\mathbb{Q}(\sqrt{-\ell})$, forcing $3 \mid \ell - 1$ and thus $3 \mid p$. But this contradicts that $p > 5$.

Now we prove that $s = 0$. If $r = 3$, the inequality $r + s \leq 3$ immediately forces $s = 0$. If $r = 1$, so that $\ell = 2p+1$, then (10) implies that $s = 0$ for all $p \geq 41$. For $5 < p < 41$, we check directly that there is no case where $\ell = 2p+1$ is prime and $h_{\mathbb{Q}(\sqrt{-\ell})}$ is a power of p.

7. Proof of Theorem 1.2: Averages of $T_{\mathrm{CM}}(d)$

7.1. **The average over odd d.** Since the results for odd d are easier to obtain, we start there.

Proof of the upper bound in Theorem 1.2(ii). Recall that $T_{\mathrm{CM}}(d) \geq 6$ for all positive integers d. Thus, from Proposition 4.2, we may assume that $T_{\mathrm{CM}}(d) = \ell^\alpha$ or $2\ell^\alpha$ for some prime $\ell \equiv 3 \pmod 4$ and some positive integer α.

For any curve achieving the maximum indicated by $T_{\mathrm{CM}}(d)$, the CM field must be $\mathbb{Q}(\sqrt{-\ell})$, for the same reason as in the proof of Theorem 1.7. Now we apply Lemma 2.3 to bound the number of possible values of $d \leq x$, given that ℓ^α divides $\#E(F)[\mathrm{tors}]$. By a calculation similar to that seen in the proof of Theorem 1.1, the number of such d is at most $100\frac{x}{h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \ell^\alpha}$. So given ℓ^α, the contribution to $\sum_{d \leq x,\ 2 \nmid d} T_{\mathrm{CM}}(d)$ from these d is at most $100\frac{x}{h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \ell^\alpha} \cdot 2\ell^\alpha = 200x/h_{\mathbb{Q}(\sqrt{-\ell})}$.

We now sum on the possibilities for ℓ^α. Since $\ell^\alpha \leq 100x$, there are $O(\log x)$ possible values of α. Moreover, the only values of ℓ that can occur are those with $\ell \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \leq 100x$. Fix a small $\epsilon > 0$. Recalling Siegel's lower bound $h_{\mathbb{Q}(\sqrt{-\ell})} \gg \ell^{1/2-\epsilon}$, we find that $\ell \leq x^{2/3+\epsilon}$ (assuming x is sufficiently large). Hence,

$$\sum_{\ell^\alpha} 200\frac{x}{h_{\mathbb{Q}(\sqrt{-\ell})}} \ll x \log x \sum_{\ell \leq x^{2/3+\epsilon}} \frac{1}{\ell^{1/2-\epsilon}} \ll x \log x \cdot (x^{2/3+\epsilon})^{1/2+\epsilon} \ll x^{4/3+2\epsilon}.$$

Since ϵ may be taken arbitrarily small, the upper bound follows. □

Proof of the lower bound in Theorem 1.2(ii). Here the main difficulty is the need to avoid double counting.

Fix a small $\epsilon > 0$. For large x, let $Y = x^{2/3-\epsilon}$, and let $\mathscr{P}_0$ be the set of primes $\ell \equiv 3 \pmod 4$ belonging to $[Y, 2Y]$. Then $\#\mathscr{P}_0 \gg Y/\log Y$. We prune the set $\mathscr{P}_0$ as follows. Let ℓ_1 be any element of $\mathscr{P}_0$. Remove from $\mathscr{P}_0$ all ℓ for which $\frac{\ell-1}{2} \mid \frac{\ell_1-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell_1})}$. Now let ℓ_2 be any remaining element, and remove all ℓ for which $\frac{\ell-1}{2} \mid \frac{\ell_2-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell_2})}$. We continue in the same way until all elements of $\mathscr{P}_0$ are exhausted. Let $\mathscr{P}$ be the set $\ell_1, \ell_2, \ell_3, \dots$. The maximal order of the divisor function (see [15, Theorem 315, p. 343]) shows that the number of primes removed at each step in the construction of $\mathscr{P}$ is smaller than $x^{\epsilon/2}$, and so $\#\mathscr{P} \geq x^{2/3-2\epsilon}$.

By construction, as ℓ ranges over $\mathscr{P}$, the products $\frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})}$ are all distinct. By genus theory, all of these products are odd. Since $\ell \leq 2Y$ and $h_{\mathbb{Q}(\sqrt{-\ell})} \leq \ell^{1/2} \log \ell$, we find that each $\frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \leq x$. Putting all of this together with Proposition 4.3,

$$\sum_{\substack{d \leq x \\ 2 \nmid d}} T_{\mathrm{CM}}(d) \geq \sum_{\ell \in \mathscr{P}} T_{\mathrm{CM}}\left(\frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})}\right) \geq \sum_{\ell \in \mathscr{P}} \ell \geq Y \cdot \#\mathscr{P} \geq x^{4/3-3\epsilon}.$$

Since ϵ can be taken arbitrarily small, we obtain the lower bound. □

7.2. **The unrestricted average.** We will use the following result.

Proposition 7.1 ([5, Theorem 1(a)])**.** *For every prime $\ell \equiv 1 \pmod 3$, there is an elliptic curve E with $j(E) = 0$ over a number field F of degree $\frac{\ell-1}{3}$, with $E(F)$ containing a point of order ℓ.*

Proof of the lower bound in Theorem 1.2(i). Immediately from Proposition 7.1,

$$\sum_{d \leq x} T_{\mathrm{CM}}(d) \geq \sum_{\substack{x < \ell \leq 3x \\ \ell \equiv 1 \pmod 3}} T_{\mathrm{CM}}\left(\frac{\ell-1}{3}\right) \geq \sum_{\substack{x < \ell \leq 3x \\ \ell \equiv 1 \pmod 3}} \ell \geq x \sum_{\substack{x < \ell \leq 3x \\ \ell \equiv 1 \pmod 3}} 1 \gg \frac{x^2}{\log x}. \quad \square$$

The proof of the upper bound is considerably more intricate. The needed methods are similar to those used by Erdős to estimate the counting function of the range of the Euler φ-function [8]. To continue, we need two further 'anatomical' results.

Lemma 7.2.

(i) *There are positive numbers C_1 and C_2 such that for all $k \in \mathbb{Z}^+$ and all real numbers $x \geq 3$, we have*

$$\#\{d \leq x \mid \omega(d) = k\} \leq C_1 \frac{x}{\log x} \frac{(\log\log x + C_2)^{k-1}}{(k-1)!}.$$

(ii) *There is a positive number C_3 such that for all $K \in \mathbb{Z}^+$ and all real numbers $x \geq 3$, we have*

$$\#\{d \leq x \mid \Omega(n) \geq K\} \leq C_3 \frac{K}{2^K} x \log x.$$

Proof. Part (i) is a classical inequality of Hardy and Ramanujan [14]. Part (ii) is taken from [13] (Exercise 05, p. 12); for details, see the proofs of Lemmas 12 and 13 in [22]. □

To prove the upper bound in Theorem 1.2(i), we will show that the mass of $T_{\mathrm{CM}}(d)$ is highly concentrated on certain arithmetically special d.

For each positive integer n, we form a set of integers $\Lambda(n)$, with definition motivated by the statement of Theorem 2.4. For each prime power ℓ^α with $\alpha \geq 2$, let

$$\Lambda(\ell^\alpha) = \{\ell^{\alpha-2}(\ell-1)(\ell+1), \ell^{\alpha-2}(\ell-1)^2, \ell^{\alpha-1}(\ell-1)\},$$

and for each prime ℓ, let

$$\Lambda(\ell) = \{\ell^2-1, (\ell-1)^2, \ell-1\}.$$

For any $n \in \mathbb{Z}^+$, let $\Lambda(n)$ be the set of integers λ that can be written in the form

$$\prod_{\ell^\alpha \| n} \lambda_{\ell^\alpha}, \tag{11}$$

where each $\lambda_{\ell^\alpha} \in \Lambda(\ell^\alpha)$.

Lemma 7.3. *Let n be a positive integer.*

(i) *The cardinality of $\Lambda(n)$ is bounded above by $3^{\omega(n)}$.*
(ii) *Each $\lambda \in \Lambda(n)$ satisfies*

$$\lambda \gg n/(\log\log(3n))^2,$$

where the implied constant is absolute.
(iii) *Each $\lambda \in \Lambda(n)$ has*

$$\Omega(\lambda) \geq \Omega(n) - 2.$$

Proof. Since $\#\Lambda(\ell^\alpha) = 3$ for each prime power ℓ^α, (i) is immediate. To prove (ii), notice that each $\lambda_{\ell^\alpha} \in \Lambda(\ell^\alpha)$ satisfies $\lambda_{\ell^\alpha} \geq \ell^\alpha(1-1/\ell)^2$. Consequently, each $\lambda \in \Lambda(n)$ is bounded below by $n\prod_{\ell|n}(1-1/\ell)^2 = \varphi(n)^2/n$. The claim now follows from the estimate $\varphi(n) \gg n/\log\log(3n)$ (see, e.g., [15, Theorem 323, p. 352]). For (iii), observe that except in the case $\ell = 2$, each $\lambda_{\ell^\alpha} \in \Lambda_{\ell^\alpha}$ has $\Omega(\lambda_{\ell^\alpha}) \geq \alpha$, and that when $\ell = 2$, we have the weaker bound $\Omega(\lambda_{\ell^\alpha}) \geq \alpha - 2$. □

Proof of the upper bound in Theorem 1.2(i). For even d, let $T'_{\mathrm{CM}}(d)$ be defined in the same way as $T_{\mathrm{CM}}(d)$, but with the extra restriction that E is defined over a degree d number field F *containing the CM field of E*. Since we can replace F by a quadratic extension F'/F containing the CM field, we have $T_{\mathrm{CM}}(d) \leq T'_{\mathrm{CM}}(2d)$ for all d. Thus, it suffices to establish the claimed upper bound for $\sum_{d\leq x} T'_{\mathrm{CM}}(2d)$. The contribution to this latter sum from values of d with $T'_{\mathrm{CM}}(2d) \leq x/\log x$ is trivially $O(x^2/\log x)$, which is acceptable for us. Since $T'_{\mathrm{CM}}(2d) \leq T_{\mathrm{CM}}(2d) \leq Cx\log\log x$ for a certain absolute constant C (see Theorem 1 of [7]), the contribution from the remaining values of d is

$$\ll x\log\log x \sum_{\substack{d\leq x \\ T'_{\mathrm{CM}}(2d) > \frac{x}{\log x}}} 1.$$

The proof of the theorem will be completed if we show that

$$\sum_{\substack{d \le x \\ T'_{\mathrm{CM}}(2d) > \frac{x}{\log x}}} 1 \le \frac{x}{(\log x)^{1+o(1)}}, \tag{12}$$

as $x \to \infty$. To this end, suppose $T'_{\mathrm{CM}}(2d) = n > x/\log x$. From Theorem 2.4, $12d$ is divisible by some $\lambda \in \Lambda(n)$. So with

$$\Lambda' := \bigcup_{\frac{x}{\log x} < n \le Cx \log\log x} \Lambda(n),$$

we see that

$$\sum_{\substack{d \le x \\ T'_{\mathrm{CM}}(2d) > \frac{x}{\log x}}} 1 \le \#\{D \le 12x : \lambda \mid D \text{ for some } \lambda \in \Lambda'\}. \tag{13}$$

We bound the right-hand side of (13) from above by considering various (possibly overlapping) cases for λ. For notational convenience, we put $X = Cx \log\log x$. We let $\epsilon > 0$ be a small, fixed parameter.

Case I: $\lambda \in \Lambda(n)$ for an $n \in (\frac{x}{\log x}, X]$ with $\omega(n) \le \eta \log\log x$, where $\eta > 0$ is a sufficiently small constant. "Sufficiently small" is allowed to depend on ϵ, and will be specified in the course of the proof.

Using the lower bound from Lemma 7.3 on the elements of $\Lambda(n)$, we see that the number of $D \le 12x$ divisible by some $\lambda \in \Lambda(n)$ is

$$\ll x \sum_{\lambda \in \Lambda(n)} \frac{1}{\lambda} \ll \frac{x}{n} (\log\log x)^2 \sum_{\lambda \in \Lambda(n)} 1 \ll \frac{x}{n} (\log\log x)^2 \cdot 3^{\omega(n)} \ll \frac{x}{n} (\log\log x)^2 (\log x)^{\eta \log 3}.$$

If we assume that $\eta < \epsilon/\log 3$, this upper bound is $O(\frac{x}{n}(\log x)^{2\epsilon})$. Thus, the total number of D that can arise in this way is

$$\ll x (\log x)^{2\epsilon} \sum_{\substack{\frac{x}{\log x} < n \le X \\ \omega(n) \le \eta \log\log x}} \frac{1}{n}. \tag{14}$$

To estimate the sum we appeal to Lemma 7.2(i). For each $T \in [x/\log x, X]$, the number of $n \le 2T$ with $\omega(n) \le \eta \log\log x$ is

$$\ll \frac{T}{\log x} \sum_{1 \le k \le \eta \log\log x} \frac{(\log\log x + O(1))^{k-1}}{(k-1)!}.$$

We can assume $\eta < \frac{1}{2}$. Then each term in the right-hand sum on k is at most half of its successor (once x is large). Hence, the sum is bounded by twice its final term. Recalling that $(k-1)! \ge ((k-1)/e)^{k-1}$, the expression in the preceding display is thus seen to be $O(T(\log x)^{\eta \log(e/\eta) - 1 + \epsilon})$. Hence,

$$\sum_{\substack{n \in [T, 2T] \\ \omega(n) \le \eta \log\log x}} \frac{1}{n} \le \frac{1}{T} \#\{n \le 2T \mid \omega(n) \le \eta \log\log x\}$$

$$\ll (\log x)^{\eta \log(e/\eta) - 1 + \epsilon}.$$

Letting T range over the $O(\log\log x)$ values of the form $T = 2^j x/\log x$, where $j \geq 0$ and $2^j x/\log x \leq X$, we find that

$$\sum_{\substack{\frac{x}{\log x} < n \leq X \\ \omega(n) \leq \eta \log\log x}} \frac{1}{n} \ll (\log x)^{\eta \log(e/\eta) - 1 + 2\epsilon}.$$

Substituting this into (14), and choosing η sufficiently small in terms of ϵ, we get that the total number of D arising in this case is $O(x(\log x)^{5\epsilon}(\log x)^{-1})$.

Case II: $\lambda \in \Lambda(n)$ for an $n \in (\frac{x}{\log x}, X]$ with $\eta \log\log x < \omega(n) < 10 \log\log x$ and

$$\sum_{\substack{\ell \mid n \\ \Omega(\ell-1) \geq 40/\eta}} 1 \leq \frac{\eta}{2} \log\log x.$$

In this case, n must be divisible by more than $\frac{\eta}{2}\log\log x$ primes ℓ with $\Omega(\ell - 1) < 40/\eta$. The number of primes ℓ up to a given height T satisfying this restriction is $O(T/(\log T)^{2+o(1)})$, as $T \to \infty$. (In [8, p. 210], this estimate is deduced from the upper bound sieve. For more precise results, see [34].) In particular, the sum of the reciprocals of such primes ℓ is bounded by a certain constant c. Thus, the number of possibilities for n is at most

$$X \sum_{k > \frac{\eta}{2}\log\log x} \frac{1}{k!} \Bigg(\sum_{\substack{\ell \leq X \\ \Omega(\ell-1) < 40/\eta}} \frac{1}{\ell} \Bigg)^k \leq X \sum_{k > \frac{\eta}{2}\log\log x} \frac{c^k}{k!}.$$

(Here we used the multinomial theorem.) Taking ratios between neighboring terms, we see that the right-hand sum is at most twice its first term (for large x). Using Stirling's formula, we find that the right-hand side is crudely bounded above by $x/(\log x)^{100}$.

Given $n \in (\frac{x}{\log x}, X]$, the number of corresponding D is

$$\begin{aligned} &\ll x \sum_{\lambda \in \Lambda(n)} \frac{1}{\lambda} \ll \frac{x}{n} (\log\log x)^2 \cdot \#\Lambda(n) \\ &\qquad \ll (\log x)^2 \cdot \#\Lambda(n) \leq (\log x)^2 \cdot 3^{10 \log\log x} \ll (\log x)^{15}. \end{aligned}$$

Summing over the $O(x/(\log x)^{100})$ possibilities for n, we see that only $O(x/(\log x)^{85})$ values of D arise in Case II.

Case III: $\lambda \in \Lambda(n)$ for an $n \in (\frac{x}{\log x}, X]$ with $\eta \log\log x < \omega(n) < 10 \log\log x$ and

$$\sum_{\substack{\ell \mid n \\ \Omega(\ell-1) \geq 40/\eta}} 1 > \frac{\eta}{2} \log\log x.$$

Let ℓ be any prime dividing n with $\Omega(\ell - 1) \geq 40/\eta$. Choose α with $\ell^\alpha \parallel n$. Since $\ell - 1$ divides each element of $\Lambda(\ell^\alpha)$, all of these elements have at least $40/\eta$ prime factors, counted with multiplicity. So from (11), each $\lambda \in \Lambda(n)$ satisfies

$$\Omega(\lambda) \geq \frac{40}{\eta} \cdot \frac{\eta}{2} \log\log x = 20 \log\log x.$$

In particular, any D divisible by a $\lambda \in \Lambda(n)$ satisfies $\Omega(D) \geq 20 \log\log x$. But Lemma 7.2(ii) implies that the number of such $D \leq 12x$ is $O(x/(\log x)^{10})$.

Case IV: $\lambda \in \Lambda(n)$ for an $n \in (\frac{x}{\log x}, X]$ with $\omega(n) \geq 10 \log\log x$.

For each prime $\ell > 2$, we have trivially that $\Omega(\ell - 1) \geq 1$. Reasoning as in Case III, we see that each $\lambda \in \Lambda(n)$ satisfies

$$\Omega(\lambda) \geq \omega(n) - 1 > 9 \log\log x.$$

Thus, any D divisible by such a λ also has $\Omega(D) > 9 \log\log x$. By another application of Lemma 7.2(ii), the number of these $D \leq 12x$ is $O(x/(\log x)^5)$.

Assembling the estimates in cases I–IV, we see that the right-hand side of (13) is $O(x(\log x)^{5\epsilon}(\log x)^{-1})$. Since $\epsilon > 0$ is arbitrary, the upper bound is proved. □

8. Proof of Theorem 1.5: Distribution of maximal torsion subgroups

Here again it is convenient to treat the upper and lower bounds separately. The upper bound uses an elementary and classical mean-value theorem of Wintner.

Proposition 8.1 ([31, Corollary 2.2, p. 50])**.** *Let $f\colon \mathbb{Z}^+ \to \mathbb{C}$, and let $g\colon \mathbb{Z}^+ \to \mathbb{C}$ be determined by the identity*

$$f(n) = \sum_{d|n} g(d) \quad \text{for all } n \in \mathbb{Z}^+.$$

If $\sum_{n=1}^{\infty} \frac{|g(n)|}{n} < \infty$, then as $x \to \infty$,

$$\sum_{n \leq x} f(n) = (\mathfrak{S} + o(1))x, \quad \text{where} \quad \mathfrak{S} := \sum_{n=1}^{\infty} \frac{g(n)}{n}.$$

Furthermore, if f is multiplicative, then $\mathfrak{S}$ can be written as a convergent Euler product:

$$\mathfrak{S} = \prod_p \left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \dots\right).$$

If G is an abelian group of order n and torsion rank at most 2, then G has a unique representation in the form $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/\frac{n}{d}\mathbb{Z}$, where $d \mid \frac{n}{d}$. So given n, the number of such groups G is given by $\tau'(n) := \sum_{d^2|n} 1$. Notice that τ' is multiplicative.

In the next lemma, we estimate asymptotically the number of abelian groups of torsion rank at most 2 and order at most y.

Lemma 8.2. *As $y \to \infty$, we have*

$$\sum_{n \leq y} \tau'(n) \sim \frac{\pi^2}{6} y.$$

Proof. We apply Proposition 8.1 with $f = \tau_0$ and $g = \mathbf{1}_\square$, where $\mathbf{1}_\square$ is the characteristic function of the square numbers. Then $\sum_{n=1}^{\infty} \frac{|g(n)|}{n} = \zeta(2) < \infty$. Since $\sum_{n=1}^{\infty} \frac{g(n)}{n} = \zeta(2) = \frac{\pi^2}{6}$, we obtain the lemma. □

Remarks 8.1.

(i) For each fixed $r \in \mathbb{Z}^+$, one can prove in a similar way that the number of abelian groups of order not exceeding y and torsion rank not exceeding r is asymptotic to $(\prod_{2 \leq k \leq r} \zeta(k))y$, as $y \to \infty$. (For a more precise estimate when $r \geq 3$, see [1].) This result dovetails with the theorem of Erdős and Szekeres

[9] that the total number of abelian groups of order at most y is asymptotically $(\prod_{k=2}^{\infty}\zeta(k))y$. Here $\prod_{k=2}^{\infty}\zeta(k) = 2.294856591\ldots$.

(ii) Fix $\alpha > 0$. Proposition 8.1 implies that $\sum_{n\le y}\tau'(n)^\alpha \sim \mathfrak{S}_\alpha y$, as $y\to\infty$, for some constant $\mathfrak{S}_\alpha$. To see this, let $f = \tau'^\alpha$, and define g by Möbius inversion, so that $g(n) = \sum_{d|n}\mu(d)\tau'(n/d)^\alpha$. In particular, $g(p) = \tau'(p)^\alpha - 1 = 0$, while for prime powers p^k with $k\ge 2$, we have the crude bounds

$$0 \le g(p^k) = \tau'(p^k)^\alpha - \tau'(p^{k-1})^\alpha \le k^\alpha.$$

Hence, $\sum_{n=1}^{\infty}\frac{|g(n)|}{n} = \prod_p\left(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\ldots\right) = \prod_p\left(1+O(\frac{1}{p^2})\right) < \infty$.

We will use this remark below.

Proof of the upper bound in Theorem 1.5. From Lemma 8.2, the number of abelian groups of order at most $x/\log x$ and torsion rank at most 2 is $O(x/\log x)$, which is negligible for our purposes. So it suffices to consider groups that are maximal for degrees $d\le x$ having $T_{\mathrm{CM}}(d) > x/\log x$. Such d have the property that $T'_{\mathrm{CM}}(2d) > x/\log x$. Given $\epsilon > 0$, we showed (see (12)) that the number of these d is at most $x/(\log x)^{1-\epsilon}$ for large x. Let $\mathscr{B}$ be the corresponding set of values of $T_{\mathrm{CM}}(d)$. Then the number of maximal torsion subgroups coming from d with $T_{\mathrm{CM}}(d) > x/\log x$ is at most $\sum_{n\in\mathscr{B}}\tau'(n)$. Hölder's inequality shows that for any positive α and β with $\frac{1}{\alpha}+\frac{1}{\beta}=1$,

$$\sum_{n\in\mathscr{B}}\tau'(n) \le \left(\sum_{n\le Cx\log\log x}\tau'(n)^\alpha\right)^{1/\alpha}\left(\sum_{n\in\mathscr{B}}1\right)^{1/\beta}.$$

Here C has the same meaning as in the proof of Theorem 1.2(i). Let $\beta = 1+\epsilon$, so $\alpha = \frac{1+\epsilon}{\epsilon}$. By the second remark following Lemma 8.2, the first sum on n is $O(x\log\log x)$. The second sum on n is $O(x/(\log x)^{1-\epsilon})$. So the above right-hand side is

$$\ll (x\log\log x)^{\frac{\epsilon}{1+\epsilon}}\cdot x^{\frac{1}{1+\epsilon}}(\log x)^{-\frac{(1-\epsilon)}{1+\epsilon}} \ll x/(\log x)^{1-3\epsilon}.$$

Since ϵ can be taken arbitrarily small, this is acceptable for us. □

The lower bound relies on a very recent 'anatomical' result of Luca, Pizzarro-Madariaga, and Pomerance.

Proposition 8.3 ([21, Theorem 3])**.** *There is a $\delta > 0$ such that: for all $u\in\mathbb{Z}^+$ and $v\in\mathbb{Z}$, there is $C(u,v) > 0$ such that for all $2\le z\le x$, the number of primes $\ell\le x$ with $u\ell+v$ having a divisor $p-1$ with $p > z$, $p\ne\ell$, and p prime is at most*

$$C(u,v)\frac{\pi(x)}{(\log z)^\delta}.$$

Proof of the lower bound in Theorem 1.5. We will prove the stronger assertion that there are $\gg x/\log x$ distinct values of $T_{\mathrm{CM}}(d)$ for $d\le x$. We consider degrees $d = \frac{\ell-1}{3}$, where $\ell\in(x/2,x]$ is a prime with $\ell\equiv 1 \pmod 3$. By the prime number theorem for progressions, there are $(\frac{1}{4}+o(1))\frac{x}{\log x}$ such primes ℓ. We will show that for all but $o(x/\log x)$ of these values of ℓ, the corresponding d is such that $T_{\mathrm{CM}}(d)$ has largest prime factor ℓ. Consequently, after discarding the $o(x/\log x)$ exceptional values of ℓ, we obtain a set of $(\frac{1}{4}+o(1))\frac{x}{\log x}$ values of d on which the map $d\mapsto T_{\mathrm{CM}}(d)$ is injective.

From Proposition 7.1, there is a CM elliptic curve E over a number field of degree d for which E has a rational point of order ℓ. So if the largest prime factor of $T_{\mathrm{CM}}(d)$ is not ℓ, then either

(i) there is a prime p dividing $T_{\mathrm{CM}}(d)$ with $p > \ell$, or
(ii) $\ell \nmid T_{\mathrm{CM}}(d)$ and $T_{\mathrm{CM}}(d) > \ell$.

Choose an F of degree d and a CM elliptic curve $E_{/F}$ with $\#E(F)[\mathrm{tors}] = T_{\mathrm{CM}}(d)$. Let K denote the CM field.

In case (i), $E(FK)$ has a point of order p. Hence, Lemma 2.3 implies that

$$p - 1 \mid w_{FK}\frac{[FK:\mathbb{Q}]}{2} \mid w_{FK}d \mid 4(\ell - 1).$$

Since $p > \ell > x/2$, Proposition 8.3 (with $u = 4$, $v = -4$) shows that there are only $O(x/(\log x)^{1+\delta})$ possibilities for ℓ. This is negligible for us.

Now suppose that we are in case (ii). To start off, we suppose additionally that $\Omega(T_{\mathrm{CM}}(d)) > 10 \log\log x$. Let $n' = \#E(FK)[\mathrm{tors}]$. Since $T_{\mathrm{CM}}(d) = \#E(F)[\mathrm{tors}] \mid n'$, we have $\Omega(n') > 10 \log\log x$. Theorem 2.4 shows that $4(\ell - 1)$ is divisible by some $\lambda \in \Lambda(n')$. So from Lemma 7.3(iii),

$$\Omega(4(\ell - 1)) \geq \Omega(\lambda) \geq \Omega(n') - 2 > 9 \log\log x$$

(for large x). But $4(\ell - 1) \leq 4x$, and from Lemma 7.2(ii) there are only $O(x/(\log x)^5)$ integers in $[1, 4x]$ with more than $9 \log\log x$ prime factors. In particular, this subcase corresponds to only $o(x/\log x)$ possible values of ℓ.

Finally, suppose $\Omega(T_{\mathrm{CM}}(d)) < 10 \log\log x$. Since we are in case (ii), the largest prime factor r of $T_{\mathrm{CM}}(d)$ satisfies

$$r \geq (T_{\mathrm{CM}}(d))^{\frac{1}{\Omega(T_{\mathrm{CM}}(d))}} > \ell^{1/10 \log\log x} > z := x^{1/20 \log\log x}.$$

Lemma 2.3 implies that $r - 1 \mid 4\ell - 4$. We know also that $r \neq \ell$. Appealing again to Proposition 8.3, we find that ℓ is restricted to a set of size $O(x(\log\log x)^{\delta}/(\log x)^{1+\delta})$. Again, this is negligible. □

Acknowledgments. We thank Robert S. Rumely for suggesting we investigate prime power Olson degrees. The exposition in §7 benefitted from talks by Carl Pomerance on the material in [8].

The first author was supported in part by NSF grant DMS-1344994 (RTG in Algebra, Algebraic Geometry, and Number Theory, at the University of Georgia). The third author is supported by NSF award DMS-1402268.

References

[1] G. Bhowmik, *Average orders of certain functions connected with arithmetic of matrices*, J. Indian Math. Soc. (N.S.) **59** (1993), 97–105.
[2] A. Bourdon, P.L. Clark, and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*, submitted, preprint at `arXiv:1501.03526 [math.NT]`.
[3] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*, J. Number Theory **130** (2010), 1241–1250.
[4] N. Childress, *Class field theory*, Universitext, Springer, New York, 2009.
[5] P.L. Clark, B. Cook, and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), 447–479.
[6] P.L. Clark, P. Corn, A. Rice, and J. Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Computation and Mathematics **17** (2014), 509–535.
[7] P.L. Clark and P. Pollack, *The truth about torsion in the CM case*, C. R. Math. Acad. Sci. Paris, to appear.

[8] P. Erdős, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quart. J. Math. **6** (1935), 205–213.
[9] P. Erdős and G. Szekeres, *Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem*, Acta Sci. Math. (Szeged) **7** (1935), 95–102.
[10] P. Erdős and S.S. Wagstaff, Jr., *The fractional parts of the Bernoulli numbers*, Illinois J. Math. **24** (1980), 104–112.
[11] K. Ford, F. Luca, and C. Pomerance, *The image of Carmichael's λ-function*, Algebra Number Theory **8** (2014), 2009–2025.
[12] R.R. Hall, *Sets of multiples*, Cambridge Tracts in Mathematics, vol. 118, Cambridge University Press, Cambridge, 1996.
[13] R.R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.
[14] G.H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n [Quart. J. Math.* **48** *(1917), 76–92]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 262–275.
[15] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.
[16] M. Hindry and J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*, C. R. Acad. Sci. Paris Sér. I Math. **329** (1999), 97–100.
[17] M. van Hoeij, *Low degree places on the modular curve $X_1(N)$*, `arXiv:1202.4355 [math.NT]`.
[18] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
[19] D. Jeon, C.H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12.
[20] H.W. Lenstra, Jr. and C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), 483–516.
[21] F. Luca, A. Pizarro-Madariaga, and C. Pomerance, *On the counting function of irregular primes*, Indag. Math. (N.S.) **26** (2015), 147–161.
[22] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, Integers **7** (2007), article #A25, 11 pages.
[23] ———, *On the range of Carmichael's universal-exponent function*, Acta Arith. **162** (2014), 289–308.
[24] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques I.H.E.S. **47** (1977), 33–186.
[25] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.
[26] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett., to appear.
[27] L.D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. **14** (1974), 195–205.
[28] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.
[29] C. Pomerance and A. Sárközy, *On homogeneous multiplicative hybrid problems in number theory*, Acta Arith. **49** (1988), 291–302.
[30] D. Prasad and C.S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **23** (2001), 1–5.
[31] W. Schwarz and J. Spilker, *Arithmetical functions*, London Mathematical Society Lecture Note Series, vol. 184, Cambridge University Press, Cambridge, 1994.
[32] A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), 241–249.
[33] A.V. Sutherland, *Torsion subgroups of elliptic curves over number fields*, preprint.
[34] N.M. Timofeev, *Hardy-Ramanujan and Halasz inequalities for shifted prime numbers*, Mat. Zametki **57** (1995), 747–764, 799 (Russian).

University of Georgia, Mathematics Department, Boyd Graduate Studies Research Center, Athens, GA 30602, USA

E-mail address: abourdon@uga.edu

E-mail address: pete@math.uga.edu

E-mail address: pollack@uga.edu